FL MGUARD 2000/4000 Gerätetausch und Migration mGuard 8 --> mGuard 10

Anwenderhinweis

Anwenderhinweis

FL MGUARD 2000/4000 - Gerätetausch und Migration mGuard 8 --> mGuard 10

AH DE MGUARD MIGRATE 10, Revision 03 2025-02-05

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Firmware-Version: mGuard 10.5.x

Mitgeltende Dokumentation (verfügbar unter phoenixcontact.net/product/<artikel-nummer>):

Release Notes

mGuard 10.5.x Firmware – Release Notes

Benutzerhandbuch „Installation und Inbetriebnahme“

UM DE HW FL MGUARD 2000/4000 – 110192_de_xx

Benutzerhandbuch „Web-based Management“:

UM DE FW MGUARD10 – 110191_de_xx

Benutzerhandbuch „Installation, Konfiguration und Benutzung des mGuard device manager (mdm)“:

UM DE MDM 1.17 – 111024_de_xx

111259_de_03

1 Gerätetausch und Migration

1.1 Migration von mGuard 8.x nach mGuard 10.x

Die Geräte der neuen FL MGUARD 2000/4000-Serie sind kompatibel zu den Geräten der vorhergehenden Serie (Vorgängermodelle mit Firmware mGuard 8.x) (siehe Tabelle 1-1).

Es ist daher möglich, ein auf dem Vorgängermodell (mGuard 8.x) erstelltes Konfigurationsprofil auf dem neuen Gerät (mGuard 10.x) zu importieren und zu aktivieren.

Die Migration bzw. der Import der Konfiguration kann dabei auf drei Wegen erfolgen:

– Import über die Weboberfläche (Kapitel 1.3.1)
– Import über SD-Karte (Kapitel 1.3.2)
– Import über „mGuard device manager (mdm)“ (siehe mdm-Benutzerhandbuch)

Für die Mehrzahl der Anwendungsfälle erfolgt die Migration direkt und ohne zusätzlichen Konfigurationsaufwand.

Tabelle 1-1 Migration der Konfiguration von kompatiblen Geräten: mGuard 8.x --> 10.5

Neue Geräte – mGuard 10	Bestellnummer	Vorgängermodelle – mGuard 8	Bestellnummer
FL MGUARD 4302 FL MGUARD 4302/KX	1357840 1696708	FL MGUARD RS4000 TX/TX (VPN) FL MGUARD RS4000 TX/TX-P	2700634 / (2200515) 2702259
FL MGUARD 4305 FL MGUARD 4305/KX	1357875 1696779	FL MGUARD RS4004 TX/DTX (VPN)	2701876 / (2701877)
FL MGUARD 2102	1357828	FL MGUARD RS2000 TX/TX VPN FL MGUARD RS2000 TX/TX-B	2700642 2702139
FL MGUARD 2105	1357850	FL MGUARD RS2005 TX VPN	2701875
FL MGUARD 4102 PCI	1441187	FL MGUARD PCI4000 VPN	2701275
FL MGUARD 4102 PCIE	1357842	FL MGUARD PCIE4000 VPN	2701278
Die rechts angegebenen Modelle stellen keine Vorgängermodelle im eigentlichen Sinn dar. Ihre Konfiguration kann allerdings trotzdem mit entsprechenden Anpassungen auf die neuen Geräte migriert werden.		FL MGUARD GT/GT (VPN)	2700197 / (2700198)
		FL MGUARD SMART2 (VPN)	2700640 / (2700639)
		FL MGUARD DELTA TX/TX (VPN)	2700967 / (2700968)
		FL MGUARD RS4000 TX/TX VPN-M	2702465

In seltenen Fällen und bei bestimmten Konfigurationen kann es notwendig sein, die bestehende Konfiguration (mGuard 8) vor einer Migration anzupassen (siehe Kapitel 1.4).

Beachten Sie, dass Konfigurationen von Geräten der FL MGUARD (RS)4000-Serie nur nach Anpassungen auf Geräte der FL MGUARD 2000-Serie migriert werden können.

1.2 Generelles Vorgehen

- Starten Sie das alte Gerät (mGuard 8).
- Sichern Sie die aktuelle Konfiguration des alten Gerätes auf einem externen Datenträger (als atv-Datei zum herunterladen oder als Konfiguration auf ECS/SD-Karte).
- Prüfen Sie, ob nicht unterstützte Funktionen aktiviert sind.
- Setzen Sie gegebenenfalls nicht unterstützte Funktionen auf Werkseinstellungen.
- Sichern und exportieren Sie die angepasste Konfiguration des alten Gerätes.
- Starten Sie das neue Gerät (mGuard 10).
- Importieren Sie die zuvor exportierte Konfiguration auf dem neuen Gerät.
- Prüfen Sie genau, ob die Konfiguration erfolgreich importiert wurde.
- Falls noch nicht geschehen: Aktivieren Sie die importierte Konfiguration auf dem neuen Gerät.
- Trennen Sie das alte Gerät von der Spannungsversorgung.
- Trennen Sie das alte Gerät vom Netzwerk.
- Trennen Sie gegebenenfalls die Servicekontakte (I/Os) des alten Gerätes.
- Verbinden Sie das neuen Gerät mit dem Netzwerk.
- Verbinden Sie gegebenenfalls die Servicekontakte (I/Os) des neuen Gerätes.
- Starten Sie das neue Gerät.

↳ Firewall-Regeln werden aktiviert.

↳ Netzwerkverbindungen und VPN-Verbindungen werden aufgebaut .

- Prüfen Sie, ob sich die Verbindungen in Ihrem Netzwerk wie erwartet verhalten.
- Entnehmen Sie gegebenenfalls die SD-Karte aus dem Gerät.

Ergebnis

↳ Die Konfiguration des alten Gerätes wurde auf dem neuen Gerät importiert und aktiviert.

↳ Alle migrierten Funktionen werden auf dem neuen Gerät wie gehabt ausgeführt.

↳ Das alte Gerät kann demontiert und außer Betrieb genommen werden (Decommissioning Mode).

Video

Der Vorgang der Gerätemigration wird in einem kurzen Video auf der Webseite von Phoenix Contact ebenfalls dargestellt.

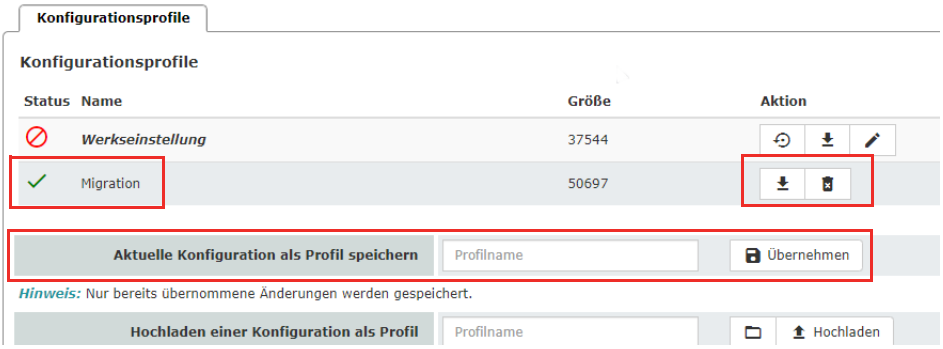
Link zum Video: phoe.co/security-router-mGuard

1.3 Gerätekonfiguration sichern und importieren

1.3.1 Import via Web-based Management (WBM)

In seltenen Fällen und bei bestimmten Konfigurationen kann es notwendig sein, die bestehende Konfiguration (mGuard 8) vor einer Migration anzupassen (siehe Kapitel 1.4).

Um eine Konfiguration über das WBM von einem mGuard 8-Gerät zu exportieren und auf einem mGuard 10.5-Gerät zu importieren, gehen Sie wie folgt vor.



Konfigurationsprofil exportieren

Erstellen und exportieren Sie zunächst ein Konfigurationsprofil auf dem alten Gerät (mGuard 8.x):

- Öffnen Sie das Menü „Verwaltung >> Konfigurationsprofile >> Konfigurationsprofile“.
- Unter „Aktuelle Konfiguration als Profil speichern“:
  - Geben Sie dem Profil einen Profilnamen.
  - Klicken Sie auf „Übernehmen“.

↪ Das Konfigurationsprofil wird in der Liste der gespeicherten Profile angezeigt.

- Klicken Sie auf den Namen des Konfigurationsprofils, das Sie migrieren wollen.

↪ Das Profil wird auf den Konfigurationsrechner heruntergeladen: *<name>.atv*

Konfigurationsprofil importieren

Importieren Sie anschließend das exportierte Konfigurationsprofil auf dem neuen Gerät (mGuard 10.5):

- Öffnen Sie das Menü „Verwaltung >> Konfigurationsprofile >> Konfigurationsprofile“.
- Unter „Hochladen einer Konfiguration als Profil“:
  - Geben Sie dem Profil einen Profilnamen.
  - Klicken Sie auf das Icon , um das zuvor erstellte Konfigurationsprofil auszuwählen.
  - Klicken Sie auf „Hochladen“.

↪ Das Konfigurationsprofil wird in das Gerät importiert und in der Liste der gespeicherten Profile angezeigt.

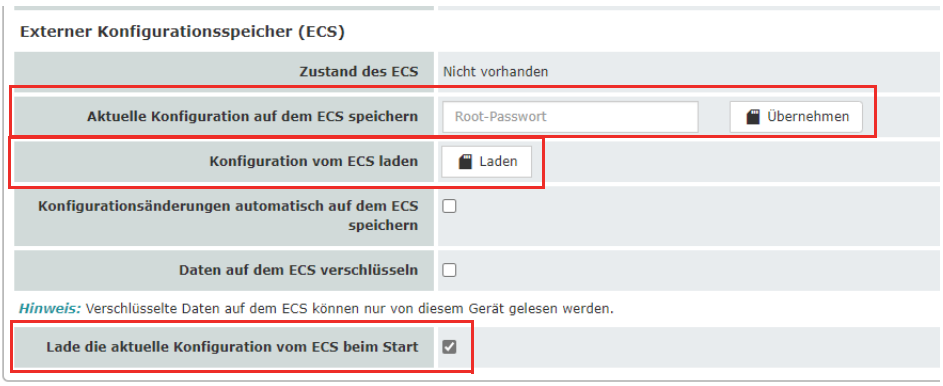
- Aktivieren Sie das Profil, indem Sie auf das Icon „Profil wiederherstellen“ klicken.

↪ Das Konfigurationsprofil wird aktiviert .

1.3.2 Import via SD-Karte (ECS)

In seltenen Fällen und bei bestimmten Konfigurationen kann es notwendig sein, die bestehende Konfiguration (mGuard 8) vor einer Migration anzupassen (siehe Kapitel 1.4).

Um eine Konfiguration via SD-Karte von einem mGuard 8-Gerät zu exportieren und auf einem mGuard 10.5-Gerät zu importieren, gehen Sie wie folgt vor.



Konfiguration exportieren

Speichern Sie die Konfiguration des alten Gerätes (mGuard 8.x) auf einer SD-Karte:

- Öffnen Sie das Menü „Verwaltung >> Konfigurationsprofile >> Externer Konfigurationsspeicher (ECS)“:
- Unter „Aktuelle Konfiguration auf dem ECS speichern“:
  - Geben Sie das Passwort des Benutzers *Root* an.
  - Klicken Sie auf die Schaltfläche „Übernehmen“.

↪ Die aktuell gespeicherte Konfiguration wird auf die eingelegte SD-Karte geschrieben.

Die Konfiguration auf dem externen Speichermedium enthält auch die verschlüsselten Passwörter (gehasht) für die Benutzer *root*, *admin*, *netadmin*, *audit* und *user* sowie für den SNMPv3-Benutzer. Diese werden beim Laden ebenfalls übernommen.

Konfiguration importieren

Der Import der Konfiguration kann auf zwei Wegen erfolgen:

1. Automatisch beim Starten

- Legen Sie die SD-Karte mit der gespeicherten Konfiguration **vor dem Start** in das neue Gerät ein.
- Starten Sie das Gerät.

↪ Die Konfiguration wird automatisch geladen und aktiviert.

2. Manuell

- Legen Sie die SD-Karten mit der gespeicherten Konfiguration **nach dem Start** in das neue Gerät ein.
- Melden Sie sich auf der Weboberfläche (WBM) des Gerätes an.
- Öffnen Sie das Menü „Verwaltung >> Konfigurationsprofile >> Externer Konfigurationsspeicher (ECS)“.
- Starten Sie die Funktion „Konfiguration vom ECS laden“.

↪ Die Konfiguration wird geladen und aktiviert.

1.3.3 Signierte Konfigurationsprofile

Ab Firmware-Version mGuard 10.5.0 ist es möglich, Konfigurationsprofile zu signieren. Auf entsprechend konfigurierten Geräten ist es dann nur noch möglich, signierte Konfigurationsprofile zu importieren und anzuwenden. Unsignierte Konfigurationen werden abgelehnt.

Möchten Sie unsignierte, bereits exportierte Konfigurationsprofile trotzdem auf einem solchen Gerät importieren, können Sie diese vor einem Import auch manuell mit einem Maschinenzertifikat des mGuard-Gerätes signieren. Das Vorgehen wird im Folgenden beschrieben.

Benötigte Dateien

Machen Sie die folgenden Dateien verfügbar.

Tabelle 1-2 Benötigte Dateien (die Namen sind beispielhaft)

my_profile.atv = Konfigurationsprofil	Konfigurationsprofil (z. B. *my_profile.atv*), das signiert werden soll.
sign.crt = Maschinenzertifikat	Maschinenzertifikat, mit dem das Konfigurationsprofil signiert werden soll. (Der zugehörige private Schlüssel ist *sign.pem*). Das Maschinenzertifikat, nicht jedoch der zugehörige private Schlüssel, kann von einem mGuard-Gerät heruntergeladen werden (oder, wie auch *sign.pem*, mittels einer abgespeicherten Datei bereitgestellt werden). Das Zertifikat muss PEM-kodiert sein. Es handelt sich um eine Textdatei. Sie beginnt mit "-----BEGIN CERTIFICATE-----".
sign.pem = privater Schlüssel	Privater Schlüssel des Maschinenzertifikats. (Das zugehörige Maschinenzertifikat ist *sign.crt*). Der private Schlüssel muss PEM-kodiert sein. Die Textdatei beginnt mit "-----BEGIN RSA PRIVATE KEY-----".

Voraussetzungen

Das Konfigurationsprofil (z. B. *my_profile.atv*)

– darf keine bereits bestehende Signatur enthalten. Zeilen, die mit "#sig" beginnen, müssen gegebenenfalls entfernt werden (siehe unten).
– muss die Unix-Konvention für Zeilenenden (einfaches „Newline“) verwenden. Falls die Datei die Windows-Konvention („Carriage Return“ gefolgt von „Newline“) verwendet, muss sie entsprechend umkodiert werden.
– muss mit einem Zeilenende-Zeichen („Newline“) enden.

Signatur erstellen

Sie können mithilfe der Dateien *sign.crt* und *sign.pem* die Signatur erstellen, mit der das Konfigurationsprofil *my_profile.atv* signiert werden soll:

- Verwenden Sie folgendes Linux-Kommando, um eine Signatur zu erstellen:

  ```
  openssl cms -sign -signer sign.crt -inkey sign.pem -in
  my_profile.atv -binary -out signature.pem -outform PEM
  ```

↪ Das Kommando erzeugt die Signatur-Datei *signature.pem*.

- Öffnen Sie die Datei *signature.pem* in einem Texteditor.
- Entfernen Sie Kopfzeile ("-----BEGIN CMS-----") und Fußzeile ("-----END CMS-----").
- Stellen Sie jeder Zeile die Textfolge "#sig", gefolgt von einem Leerzeichen voran. Verwenden Sie hierzu das folgende Linux-Kommando (inklusive aller Leerzeichen):

  ```
  sed '/^-/d; s/^/#sig /' signature.pem > signature.txt
  ```

↪ Die geänderte Datei wird in der neuen Datei *signature.txt* gespeichert.

Konfigurationsprofil signieren

Sie können mit der erstellten Signatur (*signature.txt*) das Konfigurationsprofil *my_profile.atv* signieren.

- Verwenden Sie dazu folgendes Linux-Kommando:

  cat signature.txt >> my_profile.atv

↪ Die Signatur wird an das Konfigurationsprofil *my_profile.atv* angehängt und dieses somit signiert.

↪ Sie können das signierte Konfigurationsprofil nun auf Geräten importieren, die nur signierte Konfigurationsprofile akzeptieren. Die entsprechenden Zertifikate zur Verifikation müssen auf diesen Geräten installiert sein (Maschinenzertifikat *sign.crt* oder entsprechende CA-Zertifikate, die mit *sign.crt* eine Kette des Vertrauens bilden).

Beispiel: ATV-Datei mit Signatur

```
[...]
VPN_TCPENCAP_LISTEN_PORT = "443"
VPN_UNIQUE_IDS = "no"
VPN_XFRM4_GC_THRESH = "2"
WWW_LANGUAGE = "de"
WWW_LEVEL = "10"
WWW_TIMEOUT = "1800"
// End of configuration profile
#sig MIIFcwYJKoZIhvcNAQcCoIIFZDCCBWACAQExDTALBglghkgBZQMEAgEwCwYJKoZI
#sig hvcNAQcBoIIC8DCCAuwwggHUoAMCAQICCDVQ08u5bnJBMA0GCSqGSIb3DQEBCwUA
#sig MC0xCzAJBgNVBAYTAmRlMQ4wDAYDVQQLEwVLQiBDQTEOMAwGA1UEAxMFS0IgQ0Ew
#sig HhcNMjQwODI4MDkyNTAwWhcNMzQwODI4MDkyNTAwWjAtMQswCQYDVQQGEwJkZTEO
#sig MAwGA1UECxMFS0IgQ0ExDjAMBgNVBAMTBUtCIENBMIIBIjANBgkqhkiG9w0BAQEF
#sig AAOCAQ8AMIIBCgKCAQEApjPzB1f6PwugA7anO+I1IS7TmrpDu3j63RGcIxahb8Yf
#sig 6SkogxzVvuQ9xzc39G5ByERKjamW7AbgnmnPHEU08d0x1WSA9XMTkTD8cXh1ih4S
#sig /K8L2edSdAunEHUkY9anCY0eC+MoGOMVA1XJOFBa1wZump91dKdoRmUfF1N4Nf3N
#sig sKkqHvwgR58dl9G66ovVhpZtqxKx0eAhsB20vg15cEdnTC7GZrWUgBoXGe0bdvwf
#sig 3NePis9b8NkzGByISGfe5L8RqpSZtfdDHO1zJzH10oBZtbK4iXa8YEUQagjGO92D
#sig R7AHxCA44ViSp1yXPPutRmKTYvOJvjGU4oH03yGkbwIDAQABoxAwDjAMBgNVHRME
#sig BTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCTtf/Y2gYjviznleUUCcqq3G82cL9c
#sig 1EutiiakDhHUT6+lVSSFYj4H9QMKHWRmD5B3nmeqqm6pwti93teol9VGQnD/5oQM
#sig c2mikMfah32lXwN0RiyAcki56ss0EAmhXcBBmgG4rbt7RRwy7KU8KsrauxeOtwP1
#sig aIAwg1luDnEEWOfYcOKCoYg7Z55pQHibfP9QYVApfJ/4w8nFKcyVloHZ2fSQNhpv
#sig azgZMU5cVugBU2cWd666amYQsb1FtEmKXDlJ2iDK4MniUR2uedUxNwbafYqBUGFQ
#sig WKMFTK+gLkiOMjDx2TYjFaqT9qPCWdpD0zx9zTURjTZlLk0UR3SyE3UcMYICSTCC
#sig AkUCAQEwOTAtMQswCQYDVQQGEwJkZTEOMAwGA1UECxMFS0IgQ0ExDjAMBgNVBAMT
#sig BUtCIENBAgg1UNPLuW5yQTALBglghkgBZQMEAgGggeQwGAYJKoZIhvcNAQkDMQsG
#sig CSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjUwMTA5MTMzNTU2WjAvBgkqhkiG
#sig 9w0BCQQxIgQgZYjoHiYvLsdilwjey6PC2Y/uOj2v6+KcSZQ0lE1AtdcweQYJKoZI
#sig hvcNAQkPMWwwajALBglghkgBZQMEASowCwYJYIZIAWUDBAEWMAsGCWCGSAFlAwQB
#sig AjAKBggqhkiG9w0DBzAOBggqhkiG9w0DAgICAIAwDQYIKoZIhvcNAwICAUAwBwYF
#sig Kw4DAgcwDQYIKoZIhvcNAwICASgwDQYJKoZIhvcNAQEBBQAEggEAFildP5txQr5S
#sig /7gkM6ORS4Ij2fHUd/+qGY6Bl2l8o6O/sVduYBBIG2xGt4OtBUAIormCzScXdMT3
#sig rTBEl13G6ec72qU1KpT0c+4eY+gdTVQLqp8qpaelU4sbFk4/SgpzyxT+M2pcOxD3
#sig Jik/yAYfkHuV/P4VsYNM0C0keK4Yb0XYUU85pAhStvCK8p4Fzekd+P9pODCx4VB/
#sig aSozgxhzz37pa1bxSowCMFAhZRgUtgieMuLEyAjQ+C0EwRqZT/zHzFmD3r0l72lw
#sig ZAvPvZGFkGk/C7VSworTa4fQwZNmIn8axP7Sx8CC/kEfrJl5DFtRY5xnDB+WXsNh
#sig hVzQQxbnGQ==
```

1.4 Fälle, die eine manuelle Anpassung erfordern

Manche Funktionen, die auf den Vorgängermodellen (mGuard 8) verfügbar sind, werden von den neuen Geräten (mGuard 10) nicht unterstützt (siehe).

Bei einer Migration über das Web-based Management würde bei dem Versuch, eine solche Konfiguration zu importieren, eine entsprechende Fehlermeldung angezeigt.

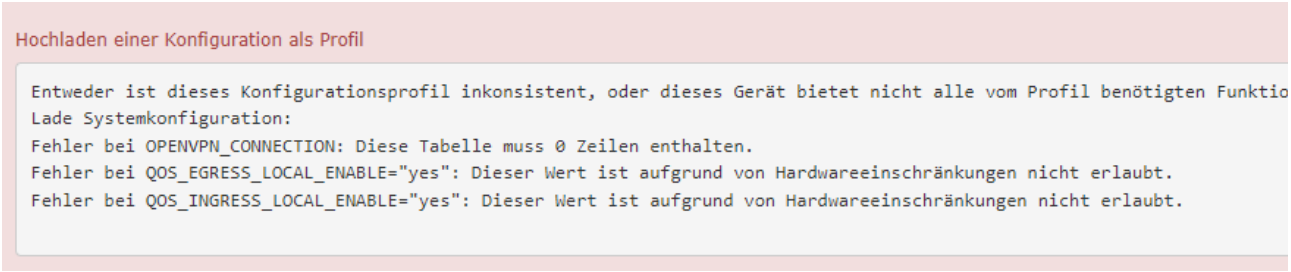


Bild 1-1 Beispiel-Fehlermeldung beim Import inkompatibler Konfigurationen

Nicht unterstützte Funktionen in mGuard 10.5

Tabelle 1-3 Nicht unterstützte Funktionen in mGuard 10.5

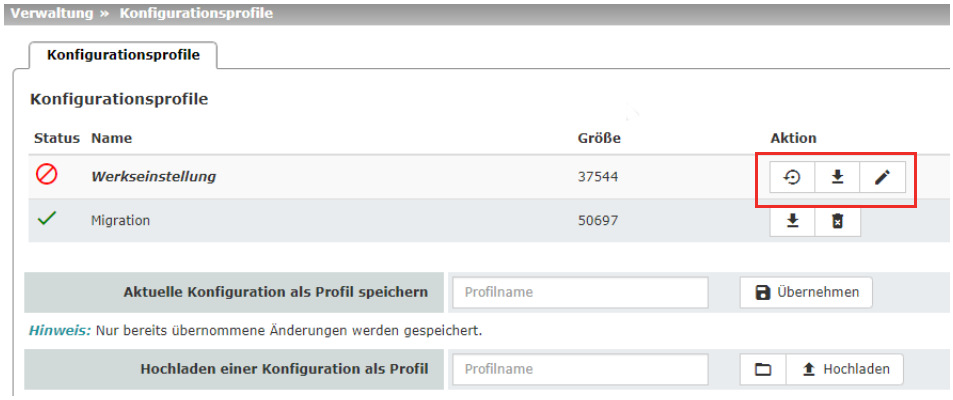
Netzwerk: Interfaces – PPPoE – PPTP – Sekundäres externes Interface
Netzwerk: Serielle Schnittstelle
Netzwerk: GRE-Tunnel (Generic Routing Encapsulation)
VPN-Redundanz
Quality of Services (QoS)
CIFS-Integrity-Monitoring
SEC-Stick

Was müssen Sie tun?

Bevor Sie die Migration starten, müssen Sie die in angegebenen Funktionen auf dem alten Gerät (mGuard 8) manuell auf Werkseinstellungen zurücksetzen. Sie können sich dabei gegebenenfalls an einer angezeigten Fehlermeldung im WBM (siehe oben) orientieren.

Gehen Sie vor, wie in Kapitel 1.5 beschrieben.

1.5 Variablen auf Werkseinstellungen zurücksetzen



Die auf dem neuen Gerät nicht mehr verfügbaren Variablen () müssen vor der Migration auf dem alten Gerät auf Werkseinstellungen zurückgesetzt werden.

Sollte dies nicht der Fall sein, wird bei einer nicht kompatiblen Konfiguration eine Fehlermeldung angezeigt, aus der Sie die anzupassenden Variablen ableiten können.

Alternativ können Sie die aktuelle Konfiguration mit den Werkseinstellungen des Gerätes vergleichen. Dies erfolgt mithilfe der „Vergleichen“-Funktion in der Web-Oberfläche.

Nachdem Sie die entsprechenden Variablen identifiziert haben, müssen Sie diese manuell auf Werkseinstellungen zurücksetzen.

Gehen Sie dazu wie folgt vor:

Erstellen Sie zunächst eine Sicherheitskopie Ihrer aktuellen Konfiguration.
Speichern Sie dazu das Konfigurationsprofil auf dem Gerät und laden Sie es herunter oder sichern Sie es auf einer SD-Karte (siehe Kapitel 1.3).

1. Melden Sie sich über das Web-based Management (WBM) auf dem Gerät an.
2. Öffen Sie das Menü „Verwaltung >> Konfigurationsprofile“.
3. Klicken Sie hinter dem Konfigurationsprofil „Werkseinstellung“ auf das Icon „Profil bearbeiten“.

↪ Das Konfigurationsprofil „Werkseinstellung“ wird geladen, aber noch nicht aktiviert.
ACHTUNG: Aktivieren Sie das Profil nicht, da sich damit die Netzwerkeinstellunge des Gerätes ändern werden und der Netzwerkzugriff verloren geht.

↪ Alle Einträge, die Änderungen zur aktuell verwendeten Konfiguration aufweisen, werden innerhalb der relevanten Seite und im zugehörigen Menüpfad grün markiert.

4. Identifizieren Sie anhand von und gegebenenfalls anhand von Fehlermeldungen im WBM die Variablen, die auf Werkseinstellungen zurückgesetzt werden müssen. Notieren Sie die entsprechenden Variablen.
5. **WICHTIG**: Stellen Sie nun Ihre **aktuell verwendete Konfiguration wieder her**, indem Sie auf das Icon „Zurücksetzen“ klicken.
6. Setzen Sie in Ihrer aktuell verwendeten Konfiguration nur die identifizierten Variablen manuell auf Werkseinstellungen zurück.
7. Klicken Sie dann auf das Icon „Übernehmen“.
8. Wiederholen Sie gegebenenfalls die Schritte 3 – 7.

↪ Wenn Sie alle relevanten Variablen auf Werkseinstellungen zurückgesetzt haben, können Sie mit der Migration beginnen (siehe Kapitel 1.3).

1.6 Geräteunterschiede

Für mehr Informationen siehe Gerätehandbuch UM DE HW FL MGUARD 2000/4000 – 110192_de_xx (verfügbar unter phoenixcontact.net/product/<artikel-nummer>).

Netzwerkports

Tabelle 1-4 Bezeichung der Netzwerkports / Switchports

mGuard 8	mGuard 10	mGuard 8 (Intern)	mGuard 10 (Intern)
WAN	XF1	(n/a)	(n/a)
LAN1	XF2	swp2	swp0
FL MGUARD 2105/4305 (KX)			
LAN2	XF3	swp0	swp1
LAN3	XF4	swp1	swp2
FL MGUARD 2105			
LAN4	XF5	swp3	swp3
FL MGUARD 4305 (KX)			
DMZ	XF5	swp4	dmz0
Nicht bei FL MGUARD 2105/FL MGUARD 4305 (KX)			
LAN5	(n/a)	swp4	(n/a)

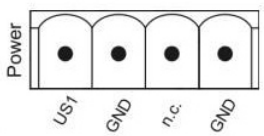
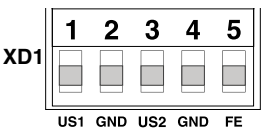
Schalteingänge / Schaltausgänge (I/Os)

Tabelle 1-5 Schalteingänge / -ausgänge (I/Os) über Combicon-Steckverbindung

mGuard 8	mGuard 10
Schalteingänge	
(Service 1) CMD1 (I1)	(XG1) CMD1 (I1)
(Service 2) CMD2 (I2)	(XG1) CMD2 (I2)
(Service) CMD3 (I3)	(XG1) CMD3 (I3)
Schaltausgänge (Meldeausgänge)	
(Service) ACK1 (O1)	(XG2) ACK1 (O1)
(Service) ACK2 (O2)	(XG2) ACK2 (O2)
Schaltausgang (Alarmausgang)	
(Contact) FAULT (O4)	(XG2) O3

Versorgungsspannung

Tabelle 1-6 Spannungsversorgung über Combicon-Steckverbindung

mGuard 8	mGuard 10 (Redundanz nur bei FL MGUARD 43xx)
	

1.6.1 Hinzugefügte Funktionen, die auf der alten Geräteplattform bereits vorhanden waren

Tabelle 1-7 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Deep Packet Inspection / Modbus TCP] **Menü:** Netzwerksicherheit >> Deep Packet Inspection >> Modbus TCP **Sektion:** Regelsätze **Variable:** diverse **GAI-Variablen:** MODBUS_RULESETS.x.FRIENDLY_NAME MODBUS_RULESETS.x.SET.y.MODBUS_FUNCTION_CODE MODBUS_RULESETS.x.SET.y.ADDRESS_RANGE MODBUS_RULESETS.x.SET.y.TARGET MODBUS_RULESETS.x.SET.y.COMMENT MODBUS_RULESETS.x.SET.y.LOG MODBUS_RULESETS.x.LOG_DEFAULT	Das mGuard-Gerät kann Pakete ein- und ausgehender Modbus-TCP-Verbindungen prüfen (*Deep Packet Inspection*) und bei Bedarf filtern. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen. Wenn bereits konfigurierte Variablenwerte vorliegen, werden diese übernommen.	**10.5.0**
[Deep Packet Inspection / OPC Inspector] **Menü:** Netzwerksicherheit >> Deep Packet Inspection >> OPC Inspector **Sektion:** OPC Inspector **Variable:** diverse **GAI-Variablen:** IP_CONNTRACK_OPC IP_CONNTRACK_OPC_SANITY IP_CONNTRACK_OPC_TIMEOUT	Die Nutzung des Netzwerk-Protokolls *OPC Classic* ist über Firewalls hinweg bislang nur möglich, wenn große Port-Bereiche geöffnet werden. Die Aktivierung der *OPC Classic*-Funktion erlaubt die einfache Nutzung dieses Netzwerk-Protokolls, ohne die Firewall des mGuard-Geräts unsicher konfigurieren zu müssen. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen. Wenn bereits konfigurierte Variablenwerte vorliegen, werden diese übernommen.	**10.5.0**

Tabelle 1-7 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Web-Zugriff über HTTPS / Server-Zertifikat] **Menü:** Verwaltung >> Web-Einstellungen >> Zugriff **Sektion:** Web-Zugriff über HTTPS **Variable:** HTTPS Server-Zertifikat **GAI-Variablen:** HTTPS_SERVER_CERT_REF In früheren Firmware-Versionen war die Funktion offiziell **nicht verfügbar**, konnte jedoch als nicht unterstützte Expertenfunktion verwendet werden.	Anstelle des auf dem mGuard-Gerät vorinstallierten selbstsignierten Webserver-Zertifikats kann ein eigenes Maschinenzertifikat auf das Gerät hochgeladen und verwendet werden. Mit diesem Zertifikat kann sich das Gerät gegenüber anfragenden Clients authentifizieren. Die Verwendung von CA-Zertifikaten in Verbindung mit einer Zertifikatskette des Vertrauens (*chain of trust*) ist möglich. **Migration von älteren mGuard-Konfigurationen** Wenn bereits ein HTTPS Server-Zertifikat verwendet wird, muss die Verwendung **vor einer Migration und vor einem Update** deaktiviert werden. Befehl auf der Kommandozeile: `gaiconfig --set HTTPS_SERVER_CERT_REF ""` Anschließend können Sie die Migration/das Update erneut ausführen und das Zertifikat (wenn es gültig ist) erneut verwenden. Wenn kein HTTPS Server-Zertifikat verwendet wird, gilt: Keine Auswirkungen.	**10.5.0**

1.6.2 Neu hinzugefügte Funktionen

Auf der neuen Geräteplattform wurden Variablen hinzugefügt, die auf der alten Geräteplattform nicht vorhanden sind.

Tabelle 1-8 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[TCP-Dump] **Menü:** Support >> Erweitert >> TCP-Dump **Sektion:** TCP-Dump **Variable (Aktion):** (1) tcpdump starten (2) tcpdump stoppen und herunterladen	Mithilfe einer Paketanalyse (*tcpdump*) kann der Inhalt von Netzwerkpaketen analysiert werden, die über ein ausgewähltes Netzwerk-Interface gesendet oder empfangen werden. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**
[Logging] **Menü:** Logging >> Einstellungen **Sektion:** Datenschutz **Variable:** Maximale Aufbewahrungsfrist für Log-Einträge **GAI-Variable:** LOGGING_MAX_DAYS	Um grundsätzliche Anforderungen an den Datenschutz zu beachten, ist es möglich, Log-Einträge nur für einen begrenzten Zeitraum auf dem Gerät zu speichern. Nach Ablauf einer konfigurierbaren Speicherfrist, werden Log-Einträge auf dem Gerät automatisch gelöscht. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Verschlüsselungsalgorithmus **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_ENCRYPTION	**Der Verschlüsselungsalgorithmus "Blowfish" wird nicht mehr unterstützt.** Insgesamt können sechs statt wie bisher drei AES-Verschlüsselungsalgorithmen ausgewählt werden: AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version mit konfiguriertem Verschlüsselungsalgorithmus „Blowfish“, wird der Wert der Variablen auf "AES-256-GCM" gesetzt. Für alle anderen Algorithmen gilt: Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsalgorithmus wird nicht geändert.	**10.5.0**

Tabelle 1-8 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[HTTPS-Zugriff] **Menü:** Verwaltung >> Web-Einstellungen >> Zugriff **Sektion:** Web-Zugriff über HTTPS **Variable:** Niedrigste unterstützte TLS-Version **GAI-Variable:** TLS_MIN_VERSION	Einige Funktionen des mGuard-Gerätes verwenden TLS-Verschlüsselung, u. a.: – Web-Server (HTTPS-Zugriff) – OpenVPN-Client Die verwendete TLS-Version wird dabei zwischen den Gegenstellen ausgehandelt. Dabei ist es möglich, dass eine nicht mehr als sicher geltende TLS-Version ausgewählt wird. Um das zu verhindern, kann ab Firmware-Version 10.5.0 festgelegt werden, welche TLS-Version als niedrigste TLS-Version vom mGuard-Gerät akzeptiert wird. Verbindungen mit niedrigeren TLS-Versionen werden vom mGuard-Gerät abgelehnt. Standard: TLS 1.2 **Migration von älteren mGuard-Konfigurationen** Die Variable wird mit dem Wert TLS 1.0/1.1 konfiguriert. Alle TLS-Versionen ab TLS 1.0 werden vom mGuard-Gerät akzeptiert.	**10.5.0**
[LINK-Modus] **Menü:** Netzwerk >> Interfaces >> Allgemein **Sektion:** Netzwerk-Status / Netzwerk-Modus **Variable:** LINK-Modus **GAI-Variable:** ROUTER_MODE_LINK	Über das bei Phoenix Contact erhältliche Gerät "CELLULINK" kann das mGuard-Gerät eine mobile Datenverbindung zu anderen Netzwerken oder dem Internet herstellen (z. B. über das 4G-Netz). Wird der LINK-Modus aktiviert, wird ein Hyperlink zum Web-based Management des Gerätes "CELLULINK" im WBM des mGuard-Gerätes angezeigt. **Migration von älteren mGuard-Konfigurationen** Keine Auswirkungen	**10.5.0**

Tabelle 1-8 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Web-Zugriff über HTTPS / Server-Zertifikat] **Menü:** Verwaltung >> Web-Einstellungen >> Zugriff **Sektion:** Web-Zugriff über HTTPS **Variable:** HTTPS Server-Zertifikat **GAI-Variablen:** HTTPS_SERVER_CERT_REF In früheren Firmware-Versionen war die Funktion offiziell **nicht verfügbar**, konnte jedoch als nicht unterstützte Expertenfunktion verwendet werden.	Anstelle des auf dem mGuard-Gerät vorinstallierten selbstsignierten Webserver-Zertifikats kann ein eigenes Maschinenzertifikat auf das Gerät hochgeladen und verwendet werden. Mit diesem Zertifikat kann sich das Gerät gegenüber anfragenden Clients authentifizieren. Die Verwendung von CA-Zertifikaten in Verbindung mit einer Zertifikatskette des Vertrauens (*chain of trust*) ist möglich. **Migration von älteren mGuard-Konfigurationen** Wenn bereits ein HTTPS Server-Zertifikat verwendet wird, muss die Verwendung **vor einer Migration und vor einem Update** deaktiviert werden. Befehl auf der Kommandozeile: `gaiconfig --set HTTPS_SERVER_CERT_REF ""` Anschließend können Sie die Migration/das Update erneut ausführen und das Zertifikat (wenn es gültig ist) erneut verwenden. Wenn kein HTTPS Server-Zertifikat verwendet wird, gilt: Keine Auswirkungen.	**10.5.0**
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Hash-Algorithmus (HMAC-Authentication) **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	Die Hash-Funktion, die zur Berechnung der Prüfsumme verwendet wird, kann konfiguriert werden. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version wird der Wert der neu hinzugefügten Variable auf "SHA-1" gesetzt.	**10.4.0**

Tabelle 1-8 Neu hinzugefügte Funktionen / Variablen / Variablenwerte

Neue Funktion / Variable /Werte	Neue Funktion / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Update-Server] **Menü:** Verwaltung >> Update >> Update **Sektion:** Update-Server **Variable:** Server-Zertifikat **GAI-Variable:** PSM_REPOSITORIES.x.REMOTE_CERT_REF	Um sicherzustellen, dass eine sichere HTTPS-Verbindung zum konfigurierten Update-Server aufgebaut wird, kann ein Server-Zertifikat des Update-Servers auf dem mGuard-Gerät installiert werden. Dieses kann vom mGuard-Gerät genutzt werden, um die Authentizität des Update-Servers zu überprüfen. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version wird der Wert der neu hinzugefügten Variable auf "Ignorieren" gesetzt.	**10.3.0**
[Alarmausgang] **Menü:** Verwaltung >> Service I/O >> Alarmausgang **Sektion:** Funktions-Überwachung **Variable:** Passwörter nicht konfiguriert **GAI-Variable:** PASSWORD_CHECK	Ein konfigurierbarer Alarm "Passwörter nicht konfiguriert" für nicht geänderte Standardpasswörter (*admin*/*root*) wurde zum Gerät hinzugefügt. Der Alarm löst den Alarmausgang über I/Os sowie die entsprechende FAIL-LED aus. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version wird der Wert der neu hinzugefügten Variable auf "Überwachen" gesetzt.	**10.3.0**

1.6.3 Geänderte Werkseinstellungen

In wenigen Fällten unterscheiden sich die Werkseinstellungen vorhandener Variablen auf der alten und der neuen Geräteplattform.

Tabelle 1-9 Geänderte Werkseinstellungen

Funktion	Geänderte Werkseinstellung / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Verschlüsselungsalgorithmus **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_ENCRYPTION	In den Werkseinstellungen wird der Verschlüsselungsalgorithmus "AES-256-GCM" statt wie bisher "AES-256-CBC" verwendet. **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version mit konfiguriertem Verschlüsselungsalgorithmus „Blowfish“, wird der Wert der Variablen auf "AES-256-GCM" gesetzt. Für alle anderen Algorithmen gilt: Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsalgorithmus wird nicht geändert.	**10.5.0**
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Hash-Algorithmus (HMAC-Authentication) **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	In den Werkseinstellungen wird der Hash-Algorithmus "SHA-256" statt wie bisher "SHA-1" verwendet. **Migration von älteren mGuard-Konfigurationen** Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Hash-Algorithmus wird nicht geändert.	**10.5.0**
[E-Mail] **Menü:** Verwaltung >> Systemeinstellungen >> E-Mail **Sektion:** E-Mail **Variable:** Verschlüsselungsmodus für den E-Mail-Server **GAI-Variable:** EMAIL_RELAY_TLS	In den Werkseinstellungen wird der Verschlüsselungsalgorithmus „TLS-Verschlüsselung“ statt wie bisher „Keine Verschlüsselung“ verwendet. **Migration von älteren mGuard-Konfigurationen** Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsmodus wird nicht geändert.	**10.5.0**

Tabelle 1-9 Geänderte Werkseinstellungen

Funktion	Geänderte Werkseinstellung / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Network Address Translation] **Menü:** Netzwerk >> NAT >> Maskierung **Sektion:** Network Address Translation/IP-Masquerading **Variable:** Ausgehend über Interface / Von IP	In den Werkseinstellungen wird eine Tabellenzeile/Regel mit den folgenden Variablen-Werten hinzugefügt: – Ausgehend über Interface: *Extern* – Von IP: *0.0.0.0/0* IP-Masquerading ist damit für alle Pakete aktiviert, die aus dem internen Netzwerk (LAN) in das externe Netzwerk (WAN) geroutet werden (LAN --> WAN). **Migration von älteren mGuard-Konfigurationen** Die Werte aus der migrierten Konfiguration werden unverändert übernommen. Eine neueTabellenzeile/Regel wird nicht hinzugefügt.	10.3.0
[Netzwerkeinstellungen] **Menü:** Netzwerk >> Interfaces >> Allgemein **Sektion:** Netzwerk-Modus **Variable:** Netzwerk-Modus	Alle Geräte der neuen Gerätegeneration werden im Netzwerk-Modus „Router“ ausgeliefert. Das externe WAN-Interface erhält seine IP-Konfiguration über DHCP. In der Werkseinstellung verhindert jedoch die Firewall den Fernzugang zum Gerät über das WAN-Interface. Über das interne LAN-Interface ist das Gerät unter der Netzwerkadresse 192.168.1.1/24 aus dem LAN-Netzwerk erreichbar. Mit dem LAN-Interface verbundene Geräte können ihre IP-Konfiguration über den DHCP-Server des mGuard-Geräts erhalten. **Migration von älteren mGuard-Konfigurationen** Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Netzwerkmodus wird nicht geändert.	10.3.0

1.6.4 Geänderte Variablenwerte

In wenigen Fällten sind Werte von Variablen auf der neuen Geräteplattform nicht mehr verfügbar und werden durch andere Werte ersetzt.

Tabelle 1-10 Geänderte Variablenwerte

Funktion	Geänderter Variablenwert / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[OpenVPN-Client] **Menü:** OpenVPN-Client > Verbindungen > Tunneleinstellungen **Sektion:** Datenverschlüsselung **Variable:** Verschlüsselungsalgorithmus **GAI-Variable:** OPENVPN_CONNECTION.x.VPN_ENCRYPTION	**Der Verschlüsselungsalgorithmus „Blowfish“ wird nicht mehr unterstützt.** Insgesamt können sechs statt bisher drei AES-Verschlüsselungsalgorithmen ausgewählt werden: AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC **Migration von älteren mGuard-Konfigurationen** Nach der Migration einer Konfiguration aus einer älteren Firmware-Version mit konfiguriertem Verschlüsselungsalgorithmus „Blowfish“, wird der Wert der Variablen auf "AES-256-GCM" gesetzt. Für alle anderen Algorithmen gilt: Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Der konfigurierte Verschlüsselungsalgorithmus wird nicht geändert.	**10.5.0**

[Shell-Zugang]
Menü: Verwaltung >> Systemeinstellungen >> Shell-Zugang
Sektion: Maximale Anzahl gleichzeitiger Sitzungen pro Rolle
Variable: Admin / Netadmin / Audit
GAI-Variablen:
SSH_ADMIN_LOGIN_ALLOWED_MAX
SSH_NETADMIN_LOGIN_ALLOWED_MAX
SSH_AUDIT_LOGIN_ALLOWED_MAX
	Die „Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ wird auf 10 begrenzt.
	Migration von älteren mGuard-Konfigurationen
	– Für alle konfigurierten Werte **<= 10** gilt:
	  – Der Wert aus der migrierten Konfiguration wird unverändert übernommen. Die konfigurierte maximale Anzahl gleichzeitiger Sitzungen pro Rolle wird nicht geändert.
	– Für alle konfigurierten Werte **> 10** gilt:
	  – Nach der Migration wird der Wert der Variable„Maximale Anzahl gleichzeitiger Sitzungen pro Rolle“ jeweils auf 10 gesetzt.
		10.5.0

Tabelle 1-10 Geänderte Variablenwerte

Funktion	Geänderter Variablenwert / Auswirkung Migration	Firmware (Eingefügt mit Firmware-Version)
[Multicast] **Menü:** Netzwerk >> Ethernet >> Multicast **Sektion:** Allgemeine Multicast-Konfiguration **Variable:** IGMP-Snooping	**Damit Daten in „Statischen Multicast-Gruppen“ korrekt an die konfigurierten Ports weitergeleitet werden, muss „IGMP-Snooping“ aktiviert werden** **Migration von älteren mGuard-Konfigurationen** Der Wert der Variable wird nach einer Migration wie folgt geändert: – **Aktiviert**: Wenn „Statischen Multicast-Gruppen“ konfiguriert sind. – **Aktiviert**: Wenn „IGMP-Snooping“ in der alten Konfiguration aktiviert ist. – **Deaktiviert**: Wenn keine „Statischen Multicast-Gruppen“ konfiguriert sind und IGMP-Snooping“ in der alten Konfiguration deaktiviert ist.	10.3.0

1.6.5 Geänderte Bezeichnungen von GAI-Variablen

Die Bezeichnung einiger GAI-Variablen wird nach der Migration von mGuard 8.x auf mGuard 10.3 oder höher geändert.

Tabelle 1-11 Geänderte Bezeichnungen von GAI-Variablen nach erfolgter Migration

GAI-Variable (mGuard 8.x)	GAI-Variable (ab mGuard 10.3)
PORT_MIRROR_RECEIVER	MIRROR_RECEIVER
PHY_SETTING	SWITCHPORT
STATIC_MULTICAST_GROUP	MULTICAST_GROUP

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Dieses Handbuch ist einschließlich aller darin enthaltenen Abbildungen urheberrechtlich geschützt. Jegliche Veränderung des Inhaltes oder eine auszugsweise Veröffentlichung sind nicht erlaubt.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:
phoenixcontact.com/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
Email: info@phoenixcontact.com
phoenixcontact.com

© Phoenix Contact 2025-02-05

111259_de_03
Item No. –03